2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) | 978-1-6654-7436-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAC3N56670.2022.10074307

Mitigating DDoS Attack using Machine Learning Approach in SDN

Ritu Raj
Reserach Scholar
Department of Computer Science
Chandigarh University
Mohali, India
ritur0059@gmail.com

Dr. Sandeep Singh Kang
Professor
Department of Computer Science
Chandigarh University
Mohali, India
sandeepkang.cse@cumail.in

***Abstract*—In the past few years, the phishing attacks have been increased exponentially which have not left any sector of the society unharmed. The most popular attack among phishing is DDoS attack in which a server is made unavailable by sending a lot of requests to the server at the same time by attacker. The reason behind these types of attacks can be anything such as demand for ransom money, revenge, competition or something else. In this research paper, we've discussed about DDoS attack and its detection techniques. A machine learning model is proposed for the detection of DDOS attack in the software defined network. The proposed model compares the accuracy, precision, recall and F1-score of various machine learning algorithms such as Logistic regression, SVM, XGBoost, Decision tree, KNN etc. The accuracy of various algorithms is predicted and on the basis of this accuracy, a detailed comparative analysis report is prepared.**

***Index Terms*—DDoS attack, DDoS detection, classification algorithms, machine learning algorithms**

I. Introduction

DoS attack is a powerful attack that makes server unavailable for it's intended users. In early times, it was very easy for a single hacker to exploit the TCP/IP protocols and take down a website. The hacker only had to send a lot of ping requests to the server until it was overwhelmed and couldn't respond resulting in shutting down the server. This was very simple for a hacker because early operating systems were not designed to handle these kind of errors. The hackers were, very well, aware about it. So, they invented different ways to exploit weaknesses in TCP/IP ICMP packet implementations. Some of them are:

(i) Sending something unexpected to the server was sufficient to take it down.
(ii) At one moment of time, even transferring packets greater than what ICMP specifications had tendency to crash a server.
(iii) Another method was to exploit TCP/IP 3-way handshake. In this method, hackers send a SYN pkt to the server pretending to initiate the conversation. The server replies back with a SYN ACK packet as an acknowledgement to the hacker. After this, hacker continues communicating with server for a moment of time and then it will leave it hanging and waiting to receive further response from hacker after getting final ACK packet from server. In the same way, hacker initiates multiple conversation and everytime leaving the server hanging and waiting for response after final ACK packet. This will fill the incoming queue of server and its limited number of open requests.

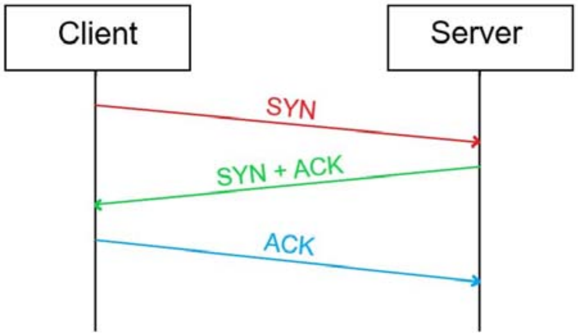


Fig. 1. 3-way Handshake

But all of the above mentioned methods no longer work for hackers now.This is because, now, the developers designs their websites that are secure against these TCP/IP errors. Poorly designed websites can still be an easy target for hackers. For instance, there is a website for buying bakery products which is poorly designed. Now, on this website if hacker searches for "a e i o u" which are basically vowels and used in almost all of the words, the server will start searching for all the words that contains vowels into its database and it'll keep searching. Basically, the server is going to return every word present in its database as a result of hacker's query. This will make the server unavailable for other users causing denial of services.

Now that developers have secured their websites against the exploitation of TCP/IP weaknesses, the hackers have also discovered new techniques to carry out DoS attack. They repeatedly request access to a particular resource and overload the web application or website by continuously reloading the

ISBN:978-1-6654-7436-8/22/$31.00 ©2022 IEEE

page, resulting in slowdown or website crash. They create delays in response to users' requests by exhausting all the bandwidth available. But with advancement in technology, a network or server is, now, able to handle DoS attack from a single source. This is no longer a problem now because DoS attack is easier to pinpoint and server can simply close the port where the hacker is attacking. But how to control a DoS attack which involves more than one source. So, now the engineers have the solution for preventing DoS attack, the hackers have also evolved their attacking technique from DoS to DDoS.

A. DDoS attack

DDoS (Distributed Denial of Service) is an evolved DoS attack in which the fraudulent requests come from more than one single source. Multiple sources are involved in DDoS attack and these sources are distributed all over the world which attack all at once on the server. Now, server has to deal with more than one source. Because of this, server will be overwhelmed and exhaust all its resources such as bandwidth, disk space or memory capacity and the legitimate users will be denied for its services. Now, the question arises, how the attacker is able to involve so many computers into DDoS attack. The attacker develops a malware software. Now, he has to install this software in other internet users' computers. For this, he infects the online websites with the malicious software or sends it as an email attachment to other users. When a user visits these infected websites or opens up the email attachment, the software gets installed in the user's computer without his knowledge. In this way, all of the infected computers that have malware installed becomes a part of an army recruited to perform attack. This army is known as Botnet. This botnet acts as an army waiting to accept instructions from its master to attack. A certain date and time is set for the attack by the attacker in malware and when the time arrives, botnet attacks simultaneously on the server and takes it down. DDoS atatck can lasts for few hours or few days depending upon attacker's intent.

B. DoS Attack Types

DoS attack is broadly classified into three major categories which cover almost all of the attacks:

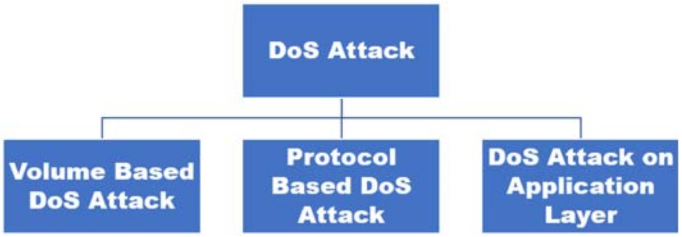


Fig. 2. DoS Attack Types

(i) Volume-based DoS attack:
These type of attacks include UDP flooding, ICMP flooding and other spoofed packets also. In this attack, the attacker directs a lot of traffic to the server so that it exhausts all its available user capacity and then becomes unable to handle legitimate users. The magnitude of these attacks is measured in bps i.e. bits per second.
(ii) Protocol-based DoS attack:
This type of attack focuses on attacking the third and fourth layer of OSI model i.e. network and transport layer respectively. Protocol based attacks basically exploits the weaknesses of transport and network layer. This type of attack includes SYN flood attack in which server starts receiving a lot of TCP connection establishment requests which overwhelms the server and makes it unavailable. This transmission rate of sending TCP connection establishment requests is measured in packets per second.
(iii) DoS attack on Application Layer:
As the name suggests, this type of attack targets the application layer. These attacks are difficult to detect because it generates legitimate traffic at very slow rate. Only highly skilled hackers and the one who have proper knowledge of working of application is capable of performing such type of attack. This attack triggers a back-end process that makes the server unresponsive.

II. Literature Review

Shreekh and Wankhede and Deepak Kshirsagar [1] proposed a system that can detect DoS attack using neural network algorithms machine learning algorithms. This approach basically detects the DoS attack at application layer, known as application layer DoS attack. CIC-IDS2017 dataset is used for this purpose that contains labeled data of year 2017 DoS and DDoS attacks generated by Hulk, Golden Eye and Slow HTTP test tools. There are total of 84 attributes in this dataset. Weka tool is used to carry out the further research. CIC-IDS2017 dataset is passed as an input to Weka tool. The experiment is performed multiple times by taking the training dataset from 20% to 80%. It is found that as we increase the number of packets in training dataset, the accuracy of detection is also increasing. The final result obtained depicts that Random Forest gives highest accuracy of 99.95% when 50% of data is used for training purpose while Multi-Layer Perceptron gives 98.87% of accuracy when 30% of data is used as training data. Hence, Random Forest gives better results than Multi-layer Perceptron algorithm.

Avinash Kumar, William Bradley Glisson and Ryan Benton [2] proposed a model that can detect attacks on a network with an accuracy rate of 81.2% . MeanShift algorithm is used for detecting the attack on KDD 99 dataset. This research proves the hypothesis that MeanShift algorithm can be used to identify network attacks in offline network traffic datasets. The KDD 99 dataset contains training data of attack of 7 weeks and testing data of 2 weeks. It has 22 different types of attacks which are classified into 4 major categories. These are: DoS, R2L attack, U2L attack and Probing attack.

Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., Silveira, L. F. [3],proposed a machine learning based approach is to detect Dos/DDoS attacks. Samples of network traffic are picked and signatures are extracted from them. On the basis of this extraction, inferences are made. Four datasets are used in the experiment which gives the high detection rate of 96% with high precision rate and low false alarm rate. The proposed system can detect high as well as low-volume DDoS attacks also. The experiment showed that the designed system gives improved Detection Rate and Precision. In case of CIC-DoS CIC-IDS 2018 datasets, the Detection Rate and Precision is higher than 93%.

Shurman, M., Khrais, R., Yateem [4] introduced two methodologies are proposed to detect Distributed Reflection DoS (DrDoS) attacks in IoT. One of the methodologies use hybrid IDS to detect IoT-DoS attack. Another methodology uses deep learning models in which LSTM is trained with latest DrDoS dataset. An IDS uses any one of the two types of approaches that is either signature based or anomaly based. Another proposed approach involves deep learning models i.e. LSTM and RNN.CIC-DDoS 2019 datatset is used for training the network. Three LSTM models are involved in this approach in which every model gives testing and training accuracy more than 90% while 3rd LSTM model gives the highest accuracy of 99.19% which is even more than Random Forest model for CIC-DDoS 2019 datatset.

M. J. Vargas-Muñoz, et.al [5] proposed a network classifier to detect usual and anomalous traffic. The introduced model defines the relationship between the various traffic features used in the dataset during feature selection. Two datasets are used for classification purpose which focuses on brute force attacks. The results are measured on the bais of false positive false negative whose value turned out to be very low. As a result, giving high efficiency for classifying normal traffic and anomalous traffic.

Won-Ju Eom, et.al [6] proposed a model to classify the normal and anomalous traffic in Software Defined Network using machine learning based approach. Four classification algorithms are used to classify the traffic and the result is measured on the basis of factors like F1 score, recall, precision and accuracy. The results of experiment demonstrated that the proposed model outperformed other existing traffic classification models and the performance of LightGBM model was the most optimal of them all.

K.S Djanie, T.E Tutu and G.J Dzisi [7] introduced a signature based Dos attack detection model using Support Vector Machine (SVM) algorithm that can detect the attack and defend the network against the DoS attacks. The network traffic is captured which is generated by various attacking tools such as Wireshark and then this traffic is analyzed. On the basis of the analysis, a model is designed that gives a high detection rate and accuracy plus low positive rate with faster detection time as compared to other existing models.

M. Zekri, Kafhali, Aboutabit and Y. Saadi[8] proposed a model for DDoS detection that can mitigate the DDoS attack using C.4.5 algorithm. This algorithm is further used with a signature detection technique which, as a result, detects the signature of DDoS attack by generating decision tree. For validation purpose, some machine learning algorithms are used and then the proposed model is compared with the result.

Naiji Zhang, Fehmi Jaafar and Yasir Malik [9] designed an algorithm which adjusts the detection rate and detection efficiency on the basis of parameters used in decision algorithms. This algorithm is a combination of ”Power Spectral Density entropy function” and SVM which helps in detecting DoS traffic from normal traffic. To achieve high efficiency, the DoS attack is detected by calculating PSD entropy and then compared witth two threshold values. This filters the 19% of obtained samples with the high detection rate. SVM is applied for minimizing the computational cost and selecting the mosts relevant detection patterns. The proposed model gives high detection rate of 99.19% and best case time complexity of O(nlogn).

Shubhra Dwivedi, Manu Vardhan and Sarsij Tripathi [10] proposed a model that can mitigate DoS attack using GOA with GOIDS, a machine learning algorithm. An IDS is designed that can distinguish the normal traffic from DoS traffic. Feature selection is done using GOIDS which selects most relevant features. Various classification techniques such as SVM, Naive Bayes, MLP and decision tree are used identify DoS attack type. KDD Cup 99 and CIC-IDS 2017 datasets are used to perform the experiment.

III. PROBLEM FORMULATION

DoS attacks have increased in the last years rapidly despite the use of many IDS and existing DoS attack detection models. In [11], K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, has proposed a machine learning model i.e. SVM and Decision Tree which detects DDoS traffic in SDN. The results show that SVM has better accuracy rate than decision tree i.e. 78% and 85%, respectively. They’ve used KDD 99 dataset for classification purpose which have many redundant values and can produce biased results.

In the proposed methodology, we are going to use to SDN specific DDoS attack dataset which is generated through mininet. The aim is to get improve the detection accuracy and detection rate.

IV. Proposed Methodology

A tool is designed using machine learning approach which classifies the malicious and legitimate traffic. Dataset is taken from Mendeley which is generated by Mininet.

Objectives acheived:
A. To study and analyze DoS and DDoS detection techniques in Software Defined Networks.
B. To propose efficient model for DDoS detection in SDN using machine learning techniques
C. To compare proposed model with existing model for DDos detection using different performance metrics.

A. Experimental setup

The datatset[20] is already present on Mendeley. The dataset is SDN specific which is produced using Mininet. The topology consists of switches and controller. The switches are connected to a single Ryu netwrok controller. Similarly, ten topologies are created in Mininet. Network simulation runs for benign TCP, UDP and ICMP traffic and malicious traffic which is the collection of TCP Syn attack, UDP Flood attack, ICMP attack. The dataset has a total of 23 features, out of which, few are obtained from switches through extraction and the remaining ones are calculated.The number of bytes transported from the switch port is denoted by tx-bytes, while the number of bytes received on the switch port is denoted by rx-bytes. The date and time are displayed in the dt field after being converted to numbers, and a flow is observed every 30 seconds.

The class attribute, which is displayed in the last column, shows whether the data is DDoS or benign. DDoS traffic is labeled as 1, while benign traffic is labeled as 0.

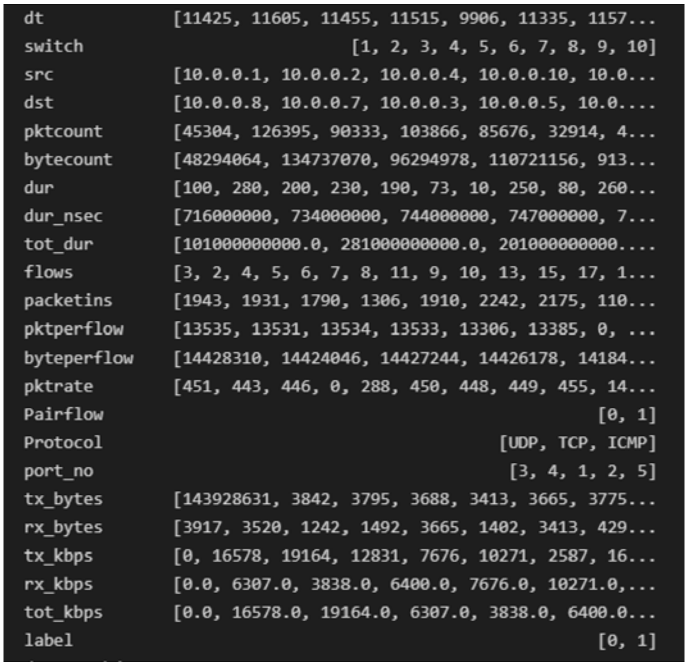
B. Approach

In the feature selection, the most relevant feature is selected for classification process. In next step, the data is passed through XGBoost, SVM, Logistic Regression, KNN and Decision tree classifier. The resulting dataset is divided into two categories: DDoS or legitimate which is depicted by 1 and 0, respectively. The controllers are informed to remove the specific flow from the flow table in the occurrence of an attack instance (flag=1). If not, the controller will build the packets' routing path for regular traffic. Whenever a DDoS issue is identified by the classifiers, the controller will send the routing tables to handle the corresponding payload.

DDOS attack detection has various phases which include data set collection and pre-processing, feature selection and classification. The steps are described below:-

Step 1: Dataset Collection: The first step is the dataset selection. So, for this purpose, the DDoS aatack SDN dataset is taken which is available on Mendeley. This dataset contains more than 1 lac rows of data and a total of 23 features are available.

Step 2: Feature Selection: In the phase of feature selection, the most relevant feature will be selected for the classification. The most relevant features mean the feature which has maximum impact on the target set. Random Forest technique is used for this purpose.



```
dt             [11425, 11605, 11455, 11515, 9906, 11335, 1157...
switch                           [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]
src            [10.0.0.1, 10.0.0.2, 10.0.0.4, 10.0.0.10, 10.0...
dst            [10.0.0.8, 10.0.0.7, 10.0.0.3, 10.0.0.5, 10.0....
pktcount       [45304, 126395, 90333, 103866, 85676, 32914, 4...
bytecount      [48294064, 134737070, 96294978, 110721156, 913...
dur            [100, 280, 200, 230, 190, 73, 10, 250, 80, 260...
dur_nsec       [716000000, 734000000, 744000000, 747000000, 7...
tot_dur        [101000000000.0, 281000000000.0, 201000000000....
flows          [3, 2, 4, 5, 6, 7, 8, 11, 9, 10, 13, 15, 17, 1...
packetins      [1943, 1931, 1790, 1306, 1910, 2242, 2175, 110...
pktperflow     [13535, 13531, 13534, 13533, 13306, 13385, 0, ...
byteperflow    [14428310, 14424046, 14427244, 14426178, 14184...
pktrate        [451, 443, 446, 0, 288, 450, 448, 449, 455, 14...
Pairflow                                                  [0, 1]
Protocol                                        [UDP, TCP, ICMP]
port_no                                          [3, 4, 1, 2, 5]
tx_bytes       [143928631, 3842, 3795, 3688, 3413, 3665, 3775...
rx_bytes       [3917, 3520, 1242, 1492, 3665, 1402, 3413, 429...
tx_kbps        [0, 16578, 19164, 12831, 7676, 10271, 2587, 16...
rx_kbps        [0.0, 6307.0, 3838.0, 6400.0, 7676.0, 10271.0,...
tot_kbps       [0.0, 16578.0, 19164.0, 6307.0, 3838.0, 6400.0...
label                                                     [0, 1]
```

Fig. 3. Numerical and Categorical Features in Dataset

Step 3: Pre-processing of data: In next phase, data is pre-processed so that it can be easily understandable to the computer. For this purpose, EDA (Exploratory Data Analysis) technique is used. The data is analyzed for its categorical or numerical value and then visualized in the form of graphs.

Step 4: Feature Encoding: In feature encoding, the categorical feature values are transformed into numerical values by assigning numeric value to each type of categories. In our dataset, we faced 3 categorical features i.e. src, dst and Protocols as shown in the figure 3. After feature encoding, dataframe has a total of 57 columns.

Step 5: Data Normalization: To prevent the redundancy of data in a database, data normalization is necessary. It is a technique of organizing data into a database in a similar fashion.

Step 6: Splitting of data: Data is divided into training and testing data. 80% of the data is used as the training data and 20% is considered as testing data. Once data is trained, it is tested against different machine learning algorithms.

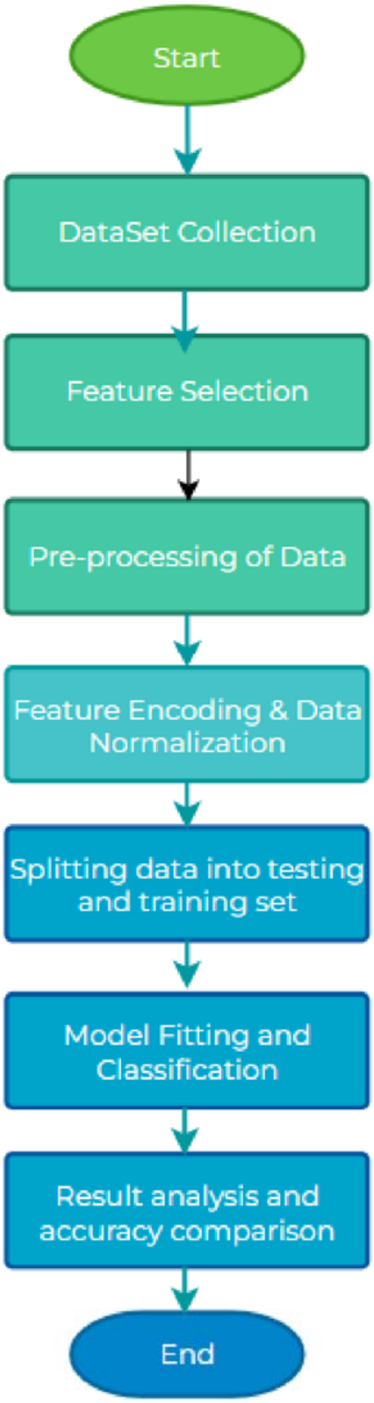

Start
DataSet Collection
Feature Selection
Pre-processing of Data
Feature Encoding & Data Normalization
Splitting data into testing and training set
Model Fitting and Classification
Result analysis and accuracy comparison
End

Fig. 4. Flowchart of steps followed

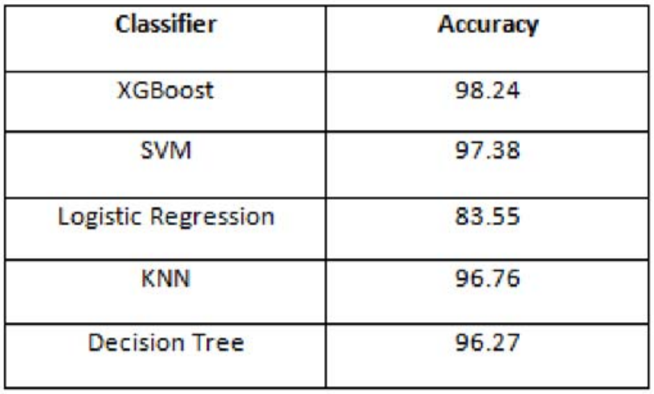
Step 7: Model Fitting: Model fitting is performed on a dataset to get more accurate and better results. Model fitting is an optimization algorithm that measures how well a machine learning model generalizes to similar data on which it is trained. The model that fits well is likely to produce more accurate results.

Step 8: Classification: A hybrid machine learning algorithm is designed which consists of multiple classifiers like KNN decision tree, support vector machine, logistic regression etc. The following algorithms are used in the proposed model:
1) Decision Tree
2) KNN (K-Nearest Neighbours
3) Logistic Regression
4) SVM (Support Vector Machine)
5) XGBoost

Step 9: Performance Analysis comparison: In this step we compare the accuracy of all the classifiers that we have obtained so far.

V. Result & Discussion

The effectiveness of any model is usually based on F1 score, precision, recall, accuracy etc. In the proposed model, we have considered accuracy, recall, precision and F1-score metrics in the end result. An SDN dataset is used in the experiment performed. The dataset is either legitimate or DDoS. The label field tells the type of data i.e. 0 if traffic is legitimate or 1 if traffic is DDoS. The categorical values are transformed into numeric after feature encoding thus, increasing the feature value to 57 in the dataset. After data normalization and model fitting, the data is fed to each model and accuracy is calculated for every classifier.



Classifier	Accuracy
XGBoost	98.24
SVM	97.38
Logistic Regression	83.55
KNN	96.76
Decision Tree	96.27

Fig. 5. Accuracy comparison

Fig. 5 shows that the XGBoost algorithm gives highest accuracy of all the algorithms used. The accuracy of XGBoost is 98.38% which is higher than the SVM model used. Logistic Regression gave the lowest accuracy of 83.84%.

After comparing the accuracy of different classifiers, we proceeded to find the value of precision and recall. The precision value for malicious traffic is 0.98 and 1 for legitimate one. Similarly, the recall for malicious traffic is 1 0.98 for legitimate traffic. The F1-score is 0.99.

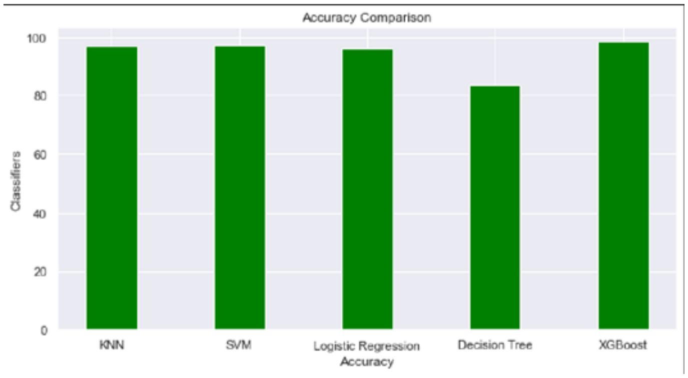
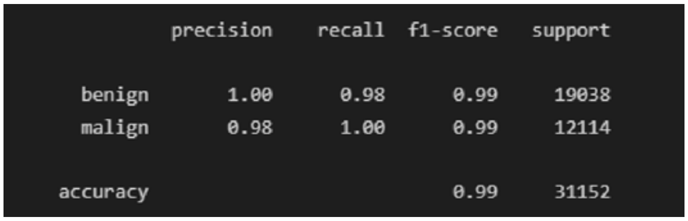


Fig. 6. Graphical Visualization of accuracies



```
              precision    recall  f1-score   support

      benign       1.00      0.98      0.99     19038
      malign       0.98      1.00      0.99     12114

    accuracy                           0.99     31152
```

Fig. 7. Precision, Recall & F1-score

VI. Conclusion & Future Scope

With the advancement in technology, different kind of threats are coming into existence such as phishing, DoS, DDoS attack etc. Detecting these kind of threats have become very difficult because they keep on evolving with time and technology. These attacks do not come with any prior warning and hence causes a lot of damage. Even if the attack once starts, people are unable to find out that this is some kind of attack. The proposed model is an approach to identify the legitimate traffic and DDoS/DoS traffic. The most suitable classification algorithm to identify the attack is XGBoost. The accuracy of all the classifiers lie between 85-98%. XGBoost is a gradient-boosting algorithm which is dominating the applied machine learning in today's world.

References

[1] Wankhede, S., Kshirsagar, D. (2018, August). DoS attack detection using machine learning and neural network. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-5). IEEE.

[2] Kumar, A., Glisson, W., Cho, H. (2020). Network attack detection using an unsupervised machine learning algorithm

[3] Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019.

[4] Shurman, M., Khrais, R., Yateem, A. (2020). DoS and DDoS attack detection using deep learning and IDS. Int. Arab J. Inf. Technol., 17(4A), 655-661.

[5] M. J. Vargas-Muñoz, R. Martínez-Peláez, P. Velarde-Alvarado, E. Moreno-García, D. L. Torres-Roman, J. J. Ceballos-Mejía, "Classification of network anomalies in flow level network traffic using Bayesian networks", 2018, International Conference on Electronics, Communications and Computers (CONIELECOMP)

[6] Won-Ju Eom, Yeong-Jun Song, Chang-Hoon Park, Jeong-Keun Kim, Geon-Hwan Kim, You-Ze Cho, "Network Traffic Classification Using Ensemble Learning in Software-Defined Networks", 2021, International Conference on Artificial Intelligence in Information and Communication (ICAIIC)

[7] Djanie, K. S., Tutu, T. E., Dzisi, G. J. (2019). A proposed DoS detection scheme for mitigating DoS attack using data mining techniques. Computers, 8(4), 85.

[8] Zekri, M., El Kafhali, S., Aboutabit, N., Saadi, Y. (2017, October). DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech) (pp. 1-7). IEEE.

[9] Zhang, N., Jaafar, F., Malik, Y. (2019, June). Low-rate DoS attack detection using PSD based entropy and machine learning. In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 59-62). IEEE.

[10] Dwivedi, S., Vardhan, M., Tripathi, S. (2022). Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. International Journal of Computers and Applications, 44(3), 219-229.

[11] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402517.

[12] V. Gomes, J. Reis, and B. Alturas, "Social engineering and the dangers of phishing," in 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020, pp. 1–7

[13] . Zabihimayvan and D. Doran, "Fuzzy rough set feature selection to enhance phishing attack detection," in 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2019, pp. 1–6.

[14] R. Almeida and C. Westphall, "Heuristic phishing detection and URL checking methodology based on scraping and web crawling," in 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), 2020, pp. 1–6.

[15] Fan Zhang, Yong Wang, Miao Ye, "Network Traffic Classification Method Based on Improved Capsule Neural Network", 2018, 14th International Conference on Computational Intelligence and Security (CIS)

[16] Xinxin Tong, Xiaobin Tan, Lingan Chen, Jian Yang, Quan Zheng, "BFSN: A Novel Method of Encrypted Traffic Classification Based on Bidirectional Flow Sequence Network", 2020, 3rd International Conference on Hot Information-Centric Networking (HotICN)

[17] S. Patil and S. Dhage, "A methodical overview on phishing detection along with an organized way to construct an anti-phishing framework," in 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), 2019, pp. 588–593.

[18] A. Abuzuraiq, M. Alkasassbeh, and M. Almseidin, "Intelligent methods for accurately detecting phishing websites," in 2020 11th International Conference on Information and Communication Systems (ICICS), 2020, pp. 085–090.

[19] N. Ahuja and G. Singal, "DDOS Attack Detection Prevention in SDN using OpenFlow Statistics," 2019 IEEE 9th International Conference on Advanced Computing (IACC), 2019, pp. 147-152, doi: 10.1109/IACC48062.2019.8971596.

[20] Ahuja, Nisha; Singal, Gaurav; Mukhopadhyay, Debajyoti (2020), "DDOS attack SDN Dataset", Mendeley Data, V1, doi: 10.17632/jxpfjc64kr.1

[21] X. You, Y. Feng and K. Sakurai, "Packet in Message Based DDoS Attack Detection in SDN Network Using OpenFlow," 2017 Fifth International Symposium on Computing and Networking (CANDAR), 2017, pp. 522-528, doi: 10.1109/CANDAR.2017.93.